Data as IP and Data License Agreements
by Daniel Glazer, Wilson Sonsini Goodrich & Rosati, Henry Lebowitz and Jason Greenberg, Fried, Frank, Harris, Shriver & Jacobson LLP, and Practical Law Intellectual Property & Technology

Encountering Data License Issues

How Data Is Protected as IP
Trade Secret Protection
Copyright Protection
Data as Intangible Property
The Computer Fraud and Abuse Act
Sui Generis Protection for Databases
Patent Protection for Databases

Approaches to Data Licensing

Data Ownership and Use
Data Ownership
Data Use

License Scope and Restrictions
License Scope
Additional License Restrictions and Obligations

Original Versus Derived Data
Derived Data: Ownership Versus Contractual Controls

Data Delivery

Data Migration and Transition
In today's technology-rich environment, companies increasingly recognize the value of data as a business asset that should be protected and can be exploited through licensing or a sale to third parties. Where one party is seeking to exploit a data feed or has developed a database it wishes to license, data issues may be the specific focus of a transaction. However, data issues also arise as an ancillary consideration in other licenses and commercial transactions, in particular technology services arrangements. Companies and their counsel can therefore encounter a range of agreements that implicate the protection and treatment of data and related intellectual property (IP) rights.

This Note discusses considerations for protecting data and data compilations, such as electronic databases, as IP and for drafting and negotiating data license agreements, including:

- How data and related IP issues are implicated in a range of agreements.
- The application of different IP regimes to the protection of data as an asset under US law.
- Potential approaches to data ownership and authorized use in data license agreements.
- Common contractual provisions in data license agreements, such as representations and warranties, indemnification, confidentiality, term and termination, and transferability.

While a party's development and use of data also may implicate privacy and data security laws relating to the collection, use, processing, and disclosure of personal information, the effect of these laws lies beyond the scope of this Note. For more on privacy and data security in the US, see Personal Information as Data and Practice Note, US Privacy and Data Security, Overview.
Encountering Data License Issues

Data issues arise in a variety of business transactions. What these transactions have in common is a party’s desire to protect and potentially exploit access to a collection of data. The underlying data, which may or may not have been generated by the owner of the compilation, has value in its aggregated form, based on, in the US, its selection criteria and organization. The protection and licensing of data may depend on:

- The nature of the data collected and the reason for its collection.
- Its manner of aggregation.

A structured data set presents an attractive option for licensing in the form of access to a database or data feed, as it may be replicated by the licensor without a loss of quality and licensed for simultaneous access by multiple parties.

Data licensing may take the form of data-specific agreements where a vendor licenses on a subscription basis a data feed or database that aggregates, for example:

- Market data.
- Consumer and business records, which may be drawn from publicly available data, such as real estate or demographic records.
- Website or search engine usage.
- Map data.
- Proprietary financial, technical, scientific, or research data.

Licensees may use these types of information for business intelligence or development, or in connection with the development of their own products and services.

Data-specific agreements also focus on data storage and processing. For example, a vendor may provide data:

- Analytics.
- De-identification.
- Cleansing.

Data issues often arise as an ancillary issue in software and other technology product and service agreements, such as license agreements, software as a service (SaaS) agreements and hosting agreements. In many of these agreements:

- The customer may need to license its customer information or data to the service provider/vendor for it to provide processing, storage, security control, back-up, or other services.
- The service provider/vendor may generate data derived from the data input and use of the services.

In these cases, it remains important that the parties address the ownership, licensing, and use of data disclosed, collected, stored, or otherwise processed under or in connection with the parties’ agreement.

How Data Is Protected as IP

In addition to protection through contractual confidentiality and restricted use provisions, a party’s data and databases may qualify for protection under one or more categories of IP, specifically:

- As a trade secret (see Trade Secret Protection).
- Under copyright (see Copyright Protection).
• As a category of intangible property (see Data as Intangible Property).
• Through database patent protection (see Patent Protection for Databases).

As with other assets protected as IP, to ensure the maximum protection for its data, a company should:

• Secure clear and verifiable chain of title, whether the compiled data is generated internally or using third-party sources.
• Consider the scope and nature of protection that may be secured:
  • under the respective IP regimes;
  • by setting up internal procedures and adopting user access (logical) and hardware, system and network (physical) security controls focused on developing and securing data and maintaining confidentiality; and
  • under contract, for example, by ensuring that the licensing of its data is consistent with the chosen protection scheme and its agreements include adequate safeguards against unauthorized use or disclosure.

Trade Secret Protection

Trade Secret Regime
Although there is no single definition of a trade secret, most states have enacted a version of the Uniform Trade Secrets Act (UTSA), which includes a trade secret definition. The federal trade secret protection statute, the Economic Espionage Act (EEA), defines "trade secret" in terms that are consistent with those set out in the UTSA (18 U.S.C. § 1839(3)), as amended by the Defend Trade Secrets Act (DTSA) (S. 1890, 114th Cong. (2015-2016)). Specifically,

• The UTSA defines "trade secret" as follows:
  "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
  (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
  (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
  (UTSA § 1(4) (1985).)
• The EEA, as amended by the DTSA, similarly provides that:
  (3) the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
  (A) the owner thereof has taken reasonable measures to keep such information secret; and
  (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]
  (18 U.S.C. § 1839(3).)
These definitions of trade secrets vary in detail, but commonly define a trade secret as information, such as a formula, pattern, compilation, program device, method, technique, or process that is both:

- **Valuable because of secrecy.** The information must be, or potentially be, economically valuable, at least in part, because it is not known or able to be discerned by others who otherwise could benefit economically from using or disclosing it.
- **Protected by efforts to maintain secrecy.** Its owner must use reasonable efforts to maintain its secrecy.

(Compare UTSA § 1(4) with 18 U.S.C. § 1839(3).)

The UTSA is model legislation that states can use to create their own state statute. The District of Columbia, Puerto Rico, the US Virgin Islands and all states, except Massachusetts and New York, have adopted a version of the UTSA model. The EEA (18 U.S.C. §§ 1831-1839) provides for federal criminal and civil actions for theft of trade secrets (18 U.S.C. §§ 1832 and 1836). However, the statute did not provide for a private right of action for trade secret misappropriation until the May 11, 2016 enactment of the DTSA (S. 1890, 114th Cong. (2015-2016)), before which private enforcement of trade secrets was governed exclusively by state law. The DTSA supplements but does not preempt state law. For an overview of the DTSA, see Legal Update, Are You Ready for the Defend Trade Secrets Act?

In most instances, states have adopted the UTSA with few or no changes. For more on the approach in specific states, see Trade Secret Laws: State Q&A Tool.

**Duration of Trade Secret Protection**

The term of protection for trade secrets is perpetual, which means that information remains a trade secret if it continues to meet the trade secret definition.

**Protecting Data as a Trade Secret**

A party seeking to acquire or retain trade secret protection for its information must use reasonable efforts to maintain the information's secrecy. To protect its data and databases as trade secrets, a party must therefore ensure that it:

- Limits the disclosure of the data solely to those employees, contractors, suppliers, vendors, business partners, and other individuals and entities that:
  - have a "need to know"; and
  - are bound by contractual, fiduciary, or other enforceable confidentiality and restricted use obligations.
- Uses adequate internal mechanisms to protect against the disclosure.

Where a company wants to protect data or databases as confidential information that is not a trade secret, it should similarly create contractual obligations with all employees and persons who will be exposed to this information. This is because there generally is limited, if any, non-contractual legal protection for confidential information that does not rise to the level of a trade secret.

**Copyright Protection**
Copyright Regime
Copyright provides its owner with a bundle of exclusive rights in an original work of authorship for the duration of the copyright. These include the right to:

- Make copies of the work.
- Distribute, perform, and display the work.
- Prepare derivative works based on the work.

A work qualifies for copyright protection under the US Copyright Act only if it has a minimal amount of creative expression (originality) and has been fixed in a tangible medium. Given these requirements, copyright does not protect underlying facts that comprise a data set, but can protect a compilation (see Protecting Data Under Copyright).

The initial owner of the copyright in a protected work is generally the work's author, unless transferred by written agreement. For works created by a single author and not as a work made for hire, the author is the person that reduces an idea to original expression and commits that expression to a tangible medium. In the context of a work made for hire, the employer or commissioning party is considered the author of the work.

For more on copyright protection, see Practice Note, Copyright: Overview.

Duration of Copyright Protection
Unlike trade secret protection, copyright protection is limited for:

- A human author, to the life of author plus 70 years.
- A corporate or other institutional author, to the earlier of 95 years from publication or 120 years from creation.

Protecting Data Under Copyright
For data to be protected under copyright, it must qualify as a compilation. While the underlying facts or data that make up a data set may not be protected under copyright, the selection and arrangement of this data can be protected if it has the required minimum level of originality.

In the seminal case *Feist Publications, Inc. v. Rural Telephone Service Co.*, the US Supreme Court ruled that a party's toil, or "sweat of the brow," in collecting information does not itself confer copyright protection on a compilation of facts. However, the Court stated that where a compilation contains a minimum amount of creativity in selection, coordination, and arrangement of data it may meet copyright's threshold originality requirement. In this case, "the resulting [compilation] as a whole constitutes an original work of authorship" (499 U.S. 340 (1991)).

As the US Court of Appeals for the Second Circuit has noted, the threshold level of originality for copyright protection is minimal and most compilations, through the compiler's independent choice in the coordination, selection, or arrangement of data, will qualify (*CCC Info. Servs., Inc. v. Maclean Hunter Mkt. Reports, Inc.*, 44 F.3d 61 (2d Cir. 1994)).
Applying these standards, courts have found, for example, the following examples of works to be copyrightable:

- A directory of Chinese-American businesses (see *Key Publ'ns v. Chinatown Today Pub. Ent.*, 945 F.2d 509 (2d Cir. 1991)).
- A baseball pitching form with nine statistical columns (see *Kregos v. Associated Press*, 937 F.2d 700 (2d Cir. 1991)).
- A compilation of wholesale prices of collectible coins (see *CDN Inc. v. Kapes*, 197 F.3d 1256 (9th Cir. 1999)).

Courts have found the following examples of works to be ineligible for copyright protection:

- A generic white pages directory (see *Feist*, 499 U.S. 340).
- A comprehensive cable system factbook (see *Warren Pub., Inc. v. Microdos Data Corp.*, 115 F.3d 1509 (11th Cir. 1997)).
- A comprehensive "Code on Dental Procedures and Nomenclature" (see *Am. Dental Ass'n v. Delta Dental Plans Ass'n*, 126 F.3d 977 (7th Cir. 1997)).

The comprehensiveness of some of these latter data collections worked against their eligibility for copyright protection. Essentially, they lacked the selectivity to be deemed original.

**Data as Intangible Property**

In the US, databases do not benefit from their own *sui generis* protection, as they do in the EU (see *Sui Generis Protection for Databases*). However, some recent US case law treats data like any other property by according it certain common law protections. Specifically, courts have extended traditional tort claims for interference with, or misappropriation of, another's tangible, personal property in the form of:

- Trespass to chattels.
- Conversion, which is usually brought in cases where the interference with the plaintiff's property is more severe, effectively depriving the plaintiff of its ownership of and access to the property.

**Trespass to Chattels**

The tort of trespass to chattels has been interpreted as covering the use of a computer system that is without or in excess of authorization, and results in demonstrable damages. This may include website scraping (see, for example, *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)) or spam e-mail (but see *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (Cal. 2003)) (not recognizing a claim of trespass to chattels because the spam did not damage or impair the plaintiff's computer system).

For example, in *Register.com, Inc. v. Verio, Inc.*, the plaintiff alleged a claim of trespass to chattels based on the defendant's use of automated bots to crawl its computer systems and access its data (356 F.3d 393 (2d Cir. 2004)). The Second Circuit upheld the grant of a preliminary injunction, finding that the repeated unauthorized intrusions could impair the "condition, quality, or value" of the plaintiff's property (in this case, its servers).

**Conversion**
In a few states, courts have recognized the tort of conversion of intangible property. This may include the unauthorized taking of information on computers and websites. For example:

- In *Thyroff v. Nationwide Mutual Insurance Co.*, the New York State Court of Appeals held that under New York law the tort of conversion must keep pace with the "contemporary realities of widespread computer use" (8 N.Y.3d 283 (N.Y. 2007)). It found that data in the form of "electronic records that were stored on a computer and were indistinguishable from printed documents" may be subject to a claim of conversion. However, the court noted that its decision was limited solely to this type of information and did not extend to all forms of virtual information.

- Following *Thyroff*, the US Bankruptcy Court of the Southern District of Texas concluded that the alleged copying of seismic data stored on a computer may be the subject of a conversion claim because the data "could not exist apart from some physical storage medium, such as a computer, flash drive, tapes, or film" and "could be accessed by a human user in a manner analogous to the access of traditional tangible property." The court also noted that although the data was stored in an electronic format for efficiency reasons, it "could have been represented through other, indisputably tangible, media" (*In re Yazoo Pipeline Co. LP*, 459 B.R. 636 (Bankr. S.D. Tex. 2011)).

However, at least one court has refused to recognize the tort of conversion of intangible property. In *Capitol Com'n, Inc. v. Capitol Ministries*, the US District Court for the Eastern District of North Carolina granted a plaintiff's motion for summary judgment dismissing the defendant's counterclaim for conversion of electronic copies of the defendant's donor lists and training manual on the grounds that "electronic data cannot be the subject of a conversion or trespass to chattels" (2013 WL 5493013 (E.D.N.C. Oct. 1, 2013)).

### The Computer Fraud and Abuse Act

Another means of protecting data and databases as intangible assets is the [Computer Fraud and Abuse Act](https://www.law.cornell.edu/uscode/text/18/part-I/chapter-100/section-1030) (CFAA). The CFAA protects:

- Any computer used in or affecting interstate commerce.
- Computers used specifically by or for the federal government or a financial institution.

Although it is a criminal statute, in certain circumstances the CFAA permits an individual who suffered damages to bring a civil action for damages or injunctive relief against a violator of the act. The plaintiff must demonstrate that:

- The defendant either:
  - "intentionally acces[s] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed] information from any protected computer" (18 U.S.C. § 1030(a)(2)(C)); or
  - "knowingly cause[d] the transmission of a program . . . and cause[d] damage without authorization to a protected computer" (18 U.S.C. § 1030(a)(5)(A)).

- The unauthorized access resulted in loss or damage during a one-year period of at least $5,000 in value (18 U.S.C. § 1030(c)(4)(A)(i)(II)). Losses may include the cost of responding to an event, conducting a damage assessment, and lost revenue due to interruption of service. However, lost license fees are not losses for this purpose.

### CFAA Case Law
The scope and coverage of the CFAA has been the subject of conflicting case law. For example, courts have varied on whether the CFAA covers obtaining access to a website in violation of the website's terms of use:

- The US District Court for the Central District of California found that scraping website data in violation of the website's terms of use may enable a plaintiff to prevail under a CFAA claim (Ticketmaster LLC v. RMG Techs., Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007)).
- The US District Court for the Eastern District of Virginia found no liability for scraping where the plaintiff failed to both:
  - show it used any technological barriers to block access; and
  - provide notice of its terms of use (Event, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927 (E.D. Va. 2010)).

There also is a circuit split on the application of the CFAA to the unauthorized accessing of a computer in violation of an employment agreement, where a departing employee misappropriates an employer's proprietary information:

- The US Court of Appeals for the Seventh Circuit has held that if an employee misappropriates confidential information stored on the employer's computer system, he breaches his duty of loyalty to his employer, which ends the agency relationship between them. The employee therefore loses authorization to access the information and can be held liable under the CFAA (Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)).
- The US Courts of Appeals for the Fourth and Ninth Circuits, meanwhile, have applied a narrow reading of the CFAA, limiting its application to situations where an individual accesses a computer or information on a computer without permission (see United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) and WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012)).

The application of the CFAA in the criminal context also has been controversial and some courts have pronounced the statute is unconstitutionally vague (see Nosal, 676 F.3d 854 and United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)).

**Sui Generis Protection for Databases**

The EU Directive 96/9/EC on the Legal Protection of Databases (Database Directive), implemented by the EU member states, provides *sui generis* protection for databases.

Article 1(2) of the Database Directive defines a database as "a collection of independent works, data or other materials which are arranged in a systematic or methodical way, and are individually accessible by electronic or other means." The *sui generis* right exists independently of the copyright, if any, in the database contents and protects the database's particular compilation of information. The main features of the *sui generis* database rights are:

- The right subsists in a database if there has been "a substantial investment in obtaining, verifying or presenting the contents of the database" (Article 7(1)).
- The right lasts for 15 years from the end of the calendar year in which the development of the database was completed (or, if the database is made available to the public before the end of this period, 15 years from the end of the calendar year in which the database was first made publicly available) (Article 10(2)).
- The author as "maker" is "the person who takes the initiative in obtaining, verifying or presenting the contents of a database" and assumes the risk of in one or more of these actions (Preamble 41). The author of a database:
  - must be based in the European Economic Area;
  - is the person who created it; and
Data as IP and Data License Agreements, Practical Law Practice Note 4-532-4243 (2017)

- is granted the exclusive rights under copyright to exploit it (Article 4(1)).
- The right is infringed if a person extracts or reuses all or a substantial part of the database contents without the owner's permission. Each member state must provide appropriate remedies for these violations (Article 12).

**Patent Protection for Databases**
A database, as a mere compilation of data, and the data that comprises a database will generally not qualify as patent eligible subject matter.

In certain circumstances, a party may be able to obtain some protection for database-oriented inventions if it meets the relevant standards for patentability, including novelty and nonobviousness.

For example, the US Court of Appeals for the Federal Circuit has allowed patent protection for computer memory containing stored data structures that made it easier and quicker to obtain data contained in the database system. The court permitted the claims as more than a mere embodiment or manipulation of abstract ideas because the "data structures impose[d] a physical organization on the data" (*In re Lowry*, 32 F.3d 1579 (Fed. Cir. 1994)).

However, a database owner should note that patent eligibility for computer-implemented technologies is an evolving area of law. For more on the key issues to consider when prosecuting patent applications and litigating patents covering these types of inventions, see Practice Note, Patent-Eligible Subject Matter.

**Approaches to Data Licensing**
Because data may be protected by one or more IP rights (see How Data Is Protected as IP), a third party's use of data requires a license from the data owner or a sublicense from a party licensed by the owner to grant sublicenses to the data. While similar in some respects to other types of IP licenses, data licenses present several unique licensing issues concerning, for example:

- Data ownership and use (see Data Ownership and Use).
- The treatment of original, derived, and usage data (see Original Versus Derived Data).

Among other reasons, this is because a party, for example, a service vendor, may:

- Receive or collect and compile data from another party, for example, a customer.
- Generate information or data from the other party's data on that other party's, or its own, behalf.

For example, in a transaction where a vendor is processing and generating data from data received from the customer in connection with the vendor's provision of services to the customer, the parties will likely have competing interests. The vendor in this case may want to:

- Analyze and use the customer data to provide services to the customer.
- Enhance its own "toolbox."
- If possible, process and aggregate the customer data for commercial exploitation by:
  - creating new products and services;
  - using the processed data to enhance its internal operations, products, or services; or
  - licensing the data to third parties.
The customer typically will want to:

- Maintain the confidentiality of its data.
- Prohibit use of the data other than for its benefit.
- Obtain access to, and if possible, ownership of, any new data sets resulting from the vendor’s processing of the customer's data.

A data license also should address the manner of delivery, maintenance, and control of the data, as well as data security policies, practices, and protocols, in particular where the data comprises personal or sensitive financial, technical, or commercial information.

**Data Ownership and Use**
In any data licensing transaction, a key negotiated point is accounting for the licensor's ownership of, and the licensee's permitted use of, the data.

**Data Ownership**
The party licensing out the data, whether it is a vendor or customer, should ensure the agreement accurately addresses its ownership of or other rights in the data by:

- Obtaining acknowledgements of its rights in the data from the licensee.
- Including in the agreement an appropriately tailored definition of the licensed data set.

Where the licensor owns the data, it should seek a specific acknowledgment from the licensee that the data provided under the agreement is the licensor's sole and exclusive property. In addition, to achieve the maximum scope of protection for its data, the licensor should seek acknowledgements that:

- The licensor has expended significant resources gathering, assembling, and compiling the data, and that the data is the valuable property of licensor.
- The data set provided under the agreement:
  - is an original compilation protected by US copyright laws; and
  - comprises and contains the trade secrets of the licensor.

In some circumstances, an appropriately narrow definition of licensed data will be appropriate. For example, in a data feed agreement where the licensee is not permitted to generate any derived data. This will help ensure:

- The licensed data is limited in scope.
- The licensor reserves the right to obtain additional fees for the usage of additional data or for additional manners of usage.

However, in a services agreement, the customer may want to use a broader definition to capture all data the vendor collects or receives directly or indirectly from the customer to perform the services and any related data resulting
from services performed by or on behalf of the vendor for the customer. In this case, the definition may help prevent ambiguity regarding the service provider's data ownership. For example, the agreement may:

- Specify that all "Customer Data" (or "Company Content") is owned by the customer and define customer data as: "all data that is owned, licensed, leased or developed by or on behalf of company, whether provided to vendor by company or provided by a third party to vendor in connection with vendor's provision of services to company, including any such data that is loaded into, or located in, any data files, tables, objects or other storage medium developed or maintained by or on behalf of vendor, including related data that results from hygiene, cleaning, and database build services performed by or on behalf of vendor."
- Provide that all derivative works of, based on, derived from or otherwise using any customer data are themselves considered to be customer data. This may cover, for example, all output, copies, reproductions, improvements, modifications, adaptations, and translations.
- Designate or allocate ownership of usage data reflecting any access to or use of the services by or on behalf of the customer or its authorized users.

**Data Use**

Both the data licensor and licensee should carefully consider legal and business considerations regarding data use.

The data licensor should consider what rights it can grant consistent with its business model. The licensor will usually seek to limit use of the data by the licensee. For example, where data is used by a vendor-licensee on behalf of a customer-licensor in a services relationship, the licensor typically:

- Prohibits the vendor from using the customer's data, except as necessary to provide the services or perform its other contractual obligations.
- Specifies which, if any, uses of the customer's data are permitted.
- Requires that the vendor maintain the confidentiality and security of the customer's data.
- Requires the vendor to promise that it will not use or attempt to use customer data in any other manner or for any other purpose.

The data licensee must consider what rights it needs and expects. It should ensure that the license is sufficiently broad to address all anticipated uses of the data. For example, a service provider that receives a license to its customer's data may seek to analyze and use customer data for the provider's own commercial benefit. It also may argue that the services depend on the provider's ancillary use of its customer's data, for example, to aggregate the data to provide data trending and analysis to its customer and similarly situated persons.

Where the customer-licensor finds the vendor-licensee's ancillary use of data to be acceptable, it should specify in the agreement:

- The scope of customer information the vendor may use.
- The permitted uses of that information.
- The licensee's promise not to make any other use of the information.
License Scope and Restrictions
The provisions in the agreement specifying the license scope and related restrictions should be tailored to address the licensor’s ownership and the manner and purpose of the licensee’s permitted use the data.

License Scope
The licensed scope, as reflected in the license grant, defines what the licensee may do with the data and may specifically address:

- Exclusivity. A data license will often be non-exclusive, granting rights to the licensee, but not precluding the licensor from reserving the same rights for itself and granting similar licenses to others. However, a license grant may also be:
  - exclusive, granting the rights to the licensee to the exclusion of all others, including the licensor; or
  - a sole license, granting rights to the licensee to the exclusion of third parties while not preventing the licensor itself from using the data. This may be appropriate where the licensor is using the data in its own business, but may not otherwise be interested in commercializing the data through a broad licensing program.

- Sublicensing, whether to affiliates or third parties. The agreement should either expressly:
  - prohibit the licensee from granting sublicenses; or
  - grant sublicensing rights to the licensee, specifying the number of levels of sublicensing or particular distribution channels permitted and including appropriate sublicensing obligations (for example, the sublicensor's responsibility for the actions of its sublicensees or prohibitions on distribution to the licensor's competitors).

- Whether and, if so, for what purposes the licensee may aggregate or modify the data or create or use other derivative data or works.

- The purposes for which the licensee may use the data, for example:
  - solely for the licensee's or the licensor's benefit;
  - solely for the purposes of providing services to the licensor; or
  - for redistribution to end users.

- Geographic or territorial restrictions (for example, on a state-, regional-, or country-wide basis), which may specifically limit data collection, processing, storage, transfer, or use.

- Licensed facilities (for example the licensed rights may be exercisable only at specific licensee premises).

- Authorized users or devices, for example, specifically identified or a specified number of users or devices that are permitted to use the data.

Additional License Restrictions and Obligations
To protect its data as an asset and its status as IP, the data licensor should include restrictions in its data agreements similar to those that typically are included in other IP licenses. These restrictions may include that, unless otherwise permitted by the agreement, the licensee may not:

- Use or exploit the data, including by reproducing, modifying, distributing, marketing, displaying, transferring, selling, renting, leasing or loaning the data. Depending on the data and industry, these restrictions may take
the form of specific restrictions (for example, that the licensee may not use the data as the basis of a financial instrument).

- Make the data accessible to unauthorized parties or publicly distribute it.
- Remove, obscure, or alter any required notice or any notice of the licensor's IP rights included as part of the data.
- Disassemble, translate, reverse engineer, or otherwise, decompile the data.
- Directly or indirectly impair, dispute, or contest the ownership, validity, or enforceability of the licensor's IP rights in the data.

If the agreement permits the licensor to redistribute data to third parties, the licensor should consider including additional obligations, such as requiring:

- Attribution or other crediting of the licensor as the source of the information.
- The licensee's pass-through of the agreement's terms and conditions to end users.

The licensor also should consider whether to include an export control provision, limiting the transfer or export of the data outside of the US, and a limitation on use for any illegal or injurious purposes.

**Original Versus Derived Data**

The parties should consider the treatment of not only the original licensed data, but also any resultant data that may be generated or otherwise derived from the licensed data during the agreement (commonly referred to as "derived data" or "resultant data"). The issue should be considered in any arrangement where the licensee may modify the licensed data, but is especially important in a services agreement, where data is generated through the provision of services. In that context, the data may be generated or otherwise derived from either or both:

- Processing the licensed data to create new data that is either:
  - sufficiently different from the original data so that the original data cannot be identified from analysis, processing, or reverse-engineering the derived data; or
  - a modification, enhancement, translation or other derivation of the original data but from which the original data may be traced.
- Monitoring the licensee's use of a provider's service (commonly referred to as usage data).

It is difficult to identify a default rule about what constitutes original as opposed to derived data and where ownership of each resides. Under copyright analysis:

- Derived data may be a derivative work of the original compilation.
- The right to create a derivative work of a copyright-protected work is exclusive to the copyright owner.

However, under trade secret analysis, there is some ambiguity about whether ownership in derived data should reside with the owner of the underlying data set that is being processed or a vendor that creates the derived data. For example:

- In *Computer Associates International, Inc. v. American Fundware, Inc.*, the court found that the common law hired–to-invent doctrine applied to the ownership of accounting software developed for a hiring company by an independent contractor and treated as a trade secret. While the court noted that from the perspective of copyright it is relevant whether a work is developed by an employee or independent contractor, it found this

- However, in *ICE Corp. v. Hamilton Sundstrand Corp.*, the US Court of Appeals for the Tenth Circuit declined to review a district court’s decision not apply the hired-to-invent doctrine on the ground that the issue of who owned the trade secrets was submitted to the jury as a question of fact (432 F. App’x 732 (10th Cir. 2011)).

Owing to the uncertainty of its ownership under applicable IP law, the ownership of derived data can be, and is most often, designated by and protected by contract. In fact, the definition and ownership status of derived data often is an extensively negotiated aspect of data license agreements.

To avoid ambiguity parties may define "Derived Data" or "Resultant Data," for example, as "any data that is derived by processing Customer Data and that is sufficiently different from the Customer Data so that such Customer Data cannot be reverse engineered or otherwise identified from analysis or further processing of such derived data."

Similarly, in the context of a SaaS or other software or data hosting or service agreement, the parties may define "Usage Data," for example, as "any data reflecting the access or use of the Services by or on behalf of Customer or any Authorized User, including any end user profile, visit, session, impression, click through or click stream data and any statistical or other analysis, information or data based on or derived from any of the foregoing."

The parties may then allocate the ownership of these multiple classes of data, for example, by:

- Expressly including or excluding them in the definition of Customer Confidential Information or Vendor Confidential Information (for example, including the Customer Data and Derived Data in the definition of Customer Confidential Information).
- Specifying that the parties are the sole and exclusive owners of their respective Confidential Information.

The parties may also:

- Define a class of vendor-developed derivative IP, for example: "'Customized Products' means any intellectual property created by or on behalf of Vendor during [or within [one/[NUMBER] year(s) after the expiration or earlier termination of] the term of the Agreement that includes Customer Confidential Information in any form or that is derived in any sense from Customer Confidential Information including without limitation, any expression of same via source code and object code and associated documentation developed or modified by Vendor."
- Designate the ownership of the vendor-developed IP and provide for any grant-back assignments or licenses.

**Derived Data: Ownership Versus Contractual Controls**

There are two ways that a party can retain rights in derived data created under an agreement:

- Providing in the agreement that the party retains ownership of this data.
- Obtaining license rights or contractual covenants from the counterparty relating to the data.

The party should consider case by case whether contractual rights to the derived data are sufficient to meet its needs, or whether ownership is either required or would be beneficial. In making this determination, the following factors may be useful to consider:

- **Privity.** If the party's rights in the derived data are grounded solely in contract, it will have difficulty enforcing its rights against a third party.
• **Injunctive relief.** If the party's rights in the derived data take the form of ownership, it may be easier for it to obtain equitable remedies, including injunctive relief, against misuse of the data.

Where control over a resultant or derived data set is particularly important, the party may also consider the following additional approaches:

• **Conditional license.** The party may expressly condition the licensee's right to create resultant or derived data on its compliance with all terms and conditions in the agreement.
• **Liquidated damages.** The party may include liquidated damages provisions for the misuse or prohibited distribution of derived data.
• **Sublicensee terms and conditions.** The party may require the licensee to have any sublicensees enter into direct terms and conditions with the licensor or require that each sublicense specify the licensor as a third-party beneficiary of specified pass-through terms and conditions.

**Data Delivery**

Any data agreement should specify the data's content, and how, when and in what format the data will be delivered. Both parties should cooperate to ensure the data will be provided in a usable format and the specific means of delivery. This may include agreement on:

• Specified communications technology platforms.
• Specific hardware or software configuration requirements. The licensee will often be required to comply with a licensor-defined specification.
• The use of encryption and a secure delivery mechanism.
• The frequency of data delivery, for example, on a real-time or periodic basis.
• Service level obligations and related rights and penalties for a failure to maintain them.
• A relationship between delivery and payment obligations.
• The party that is to bear the risk of loss during transmission.
• The licensor's right to add or delete data sets and any related notice requirements.

The data licensee may require the data licensor to provide certain installation services, or training in the use of the data. In this case, the agreement should include provisions covering the provision of services, including a timetable and applicable fees (see **Consideration and Payment Terms**).

**Data Migration and Transition**

Where the agreement involves the creation of any new or derived data by a service provider or other licensee, the licensor should consider whether to include:

• Periodic delivery of the new or derived data.
• On the data licensor's request or the termination or expiration of the agreement, the data licensee's obligation to:
  • deliver all or the most recent backup of the data and prescribing the method of doing so;
  • return the licensor's data in both the licensee's data format and a platform-agnostic format and destroy all remaining licensor information on its servers; and
• provide, for a stated fee, temporary storage of the data and transition or migration assistance, including allocation of costs.

Similarly, where a party is transferring or migrating data to a new service provider for processing, the service agreement should account for any required conversion services. For example, a service provider may need to convert customer data that is being migrated from the customer's legacy or other service provider's systems.

**Data Security and Controls**

The data licensor should ensure that the licensee has adequate security controls in place to protect the licensed data and comply with applicable laws and regulations. While security requirements are important in all cases to protect data from being stolen, misused, tampered with, corrupted, or destroyed, they are critical where the data includes personal information (see Personal Information as Data).

The agreement may specify:

• Types of controls and data security to be used by the licensee including, for a service provider, the provider's data center and service network. This may be represented in a written security policy that meets or exceeds the licensor's own security standards or best industry practices and that can be attached as a schedule to the agreement.

• The obligation to be and remain in compliance with applicable data security laws and regulations and, if applicable, professional obligations affecting persons with data in particular industries and professions, such as attorneys, healthcare providers, securities brokers, and dealers.

• Procedures and obligations for data security breaches and related investigations, including obligations to:
  • notify the licensor of any detected security breaches or unauthorized access concerning any data and, in particular, data that includes personal information; and
  • provide assistance in investigating security breaches and obtaining the return of misappropriated data and other appropriate remedies.

• The parties' data transfer, communications, and encryption protocols.

For sample data security provisions, see Standard Clauses, Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer) and Standard Document, Software as a Service (SaaS) Agreement (Pro-Customer): Security.

**Audit Rights**

The data licensor should include auditing provisions to ensure that the data is being used in accordance with the license terms. This may include the right to enter the licensee's premises to inspect its data handling and use or, where possible, to access the licensee's systems remotely. The agreement should include appropriate record-keeping obligations for the licensee, both during and for a period after the termination or expiration of the agreement.

Where data security is critical, the licensor also may seek the right to audit the provider's data security capabilities through a third party's physical visit or an industry-approved audit process at the licensor's request or where circumstances make an audit necessary.
If the licensed data includes financial or other sensitive information, it may also be appropriate for the agreement to include joint security testing, including penetration testing. Penetration testing simulates attempts at unauthorized internal or external access to the tested party's systems to detect potential security weaknesses.

The licensee should seek to limit the licensor's audit rights to avoid disruption to the licensee's business (for example, by specifying that audits may be conducted no more than once in any 12-month period).

**Personal Information as Data**
Certain types of data, such as employee records and customer financial accounts, are personal information that may be subject to special requirements under various federal, state, and non-US privacy and data protection laws. For example, the following laws may impose additional obligations on the parties:

- The **Gramm-Leach-Bliley Act** (GLBA).
- The **Health Insurance Portability and Accountability Act** (HIPAA).
- The **Health Information Technology for Economic and Clinical Health Act** (HITECH).
- The **Fair Credit Reporting Act** (FCRA).
- The **Children's Online Privacy Protection Act** (COPPA).

In addition, Massachusetts and several other states have adopted regulations covering personally-identifiable information. For more information on these and other privacy and data security laws, see [Practice Note, US Privacy and Data Security: Overview](#).

Where sensitive information is provided or generated as part of a data arrangement, the party who owns the data should include:

- Robust confidentiality provisions.
- Specific obligations that the party using the data comply with all applicable laws and regulations in protecting the confidentiality of the data and refrain from unlawful use and disclosure.

Because privacy and data security obligations vary by jurisdiction, the licensor should consider prohibiting or restricting any transfer of data to another jurisdiction that raises additional data protection issues. In particular, the licensor should consider whether the data will be transmitted to the EU or includes information concerning EU residents. These considerations may be especially relevant for agreements with service providers that outsource storage or processing of customer data to employees and subcontractors in other jurisdictions to reduce costs.

If the licensee will not receive personal information, it can consider including a provision expressly prohibiting the disclosure of this information to it and requiring the redaction of all such information from the licensed materials.

**Consideration and Payment Terms**
As in other types of licenses, the financial terms of a data license agreement will vary based on the particular transaction, including the type of data licensed.
In some cases, payments may be triggered by the delivery of data, either at the onset of the transaction or on a periodic basis. In cases where the services are offered on a subscription basis, the license fee may be presented as an annual fee that increases on the renewal of the agreement.

If data is licensed as part of a services arrangement, the consideration and payment terms for the services that are provided will likely be the focus of the transaction. However, the agreement may still specify financial terms for data storage, conversion, migration and processing.

If the data licensee requires the data licensor to provide any installation or configuration services or training in the use of the data, these services also should be reflected in the licensor’s fees.

**Risk Allocation**

The parties to a data license agreement typically allocate risks in the agreement through:

- Disclaimers and representations and warranties (see Disclaimers and Representations and Warranties).
- Indemnification and limitation of liability provisions (see Indemnification and Limitations on Liability).

**Disclaimers and Representations and Warranties**

Because of the uncertainty of protecting data as IP and the nature of licensed data as an aggregated asset, a licensor may be unwilling to provide and may include an express disclaimer of representations and warranties concerning the licensed data and its use. The data licensor may seek to include the following disclaimers, particularly where the data is licensed to many licensees under a form agreement:

- The data is licensed "as is" and "as available," without any warranty of any kind, whether express or implied (including the warranties of merchantability and fitness for a particular purpose) and the licensor does not assume any responsibility for the use of the licensed data.
- The licensor provides no representations or warranties about the accuracy, completeness, authenticity, usefulness, timeliness, reliability, appropriateness, or sequencing of the data.
- The licensor does not represent or warrant the data or access to it will be uninterrupted or error-free, or that errors will be corrected.
- The licensor disclaims any obligation or liability for any data-related damages.

The agreement also may not include representations from the licensor covering the enforceability and validity of the data as IP, as may appear in other license agreements.

Where possible, the data licensee should still seek basic representations and warranties regarding the licensor's ownership interest in or other basis for its control of the data and ability to grant the license to the data set out in the agreement. Depending on the nature of the licensed data and the licensor's control, the licensee may also seek data-specific representations and warranties, for example:

- That the licensor has undertaken reasonable efforts to ensure the data's timeliness and accuracy.
- Alternatively, that the licensor will use reasonable efforts to notify the licensee of known errors.
In some cases, the licensee may be able to include one or more of these representations subject to knowledge and materiality qualifiers to make them acceptable to the licensor.

Whether or not the licensor is willing to give any representations covering the data, to reduce risk, the licensee may seek indemnification from the licensor for third-party claims resulting from the use of the licensed data for permitted purposes (see Indemnification and Limitations on Liability).

**Indemnification and Limitations on Liability**

A data license agreement may include an indemnity provision that requires each party to defend and indemnify the other party against certain claims, for example, third-party claims resulting from the other party's breach of the agreement.

The data licensee will also want to ensure that it is contractually protected if the data licensor does not have the rights to license the data. It should therefore seek to include an indemnification for third-party IP infringement claims based on the licensee's permitted use of the data.

Each party is likely to seek limitations on liability in the form of:

- A liability cap. For example, a data licensor may seek to limit its liability to the amount of fees paid to it under the agreement.
- An exclusion of damages for lost data, profits, business and reputation, and any indirect, special, punitive or consequential damages.

The parties also should consider whether to include certain exceptions to these limitations, for example:

- Indemnification obligations, in particular, for infringement.
- Breaches of confidentiality, privacy, or data security.
- Violations of applicable law.
- Damage to tangible property.
- Personal injury or death.
- Gross negligence and willful misconduct, recovery of damages for which may not be limited in certain states, such as New York.

The inclusion of these exceptions typically depends on the parties' relative bargaining power.

**Other Key Provisions**

Other important standard provisions in a data license agreement typically include:

- Term and termination (see Term and Termination).
- Confidentiality (see Confidentiality).
- Transferability of the agreement (see Assignment and Transferability).

In addition, a data license agreement usually includes standard contract boilerplate provisions, see Standard Clauses, Boilerplate Clauses.
Term
The term of a data license agreement largely will depend on the nature of the transaction and licensed data. For example:

- A data-specific agreement may have a term that is renewable on a periodic basis, such as annually.
- The term of a data license included as a part of an SaaS or other services agreement or another IP license may be coterminous with the term of the services or the services agreement or IP license.

In a data-specific agreement, where the data licensee is a customer receiving the licensor’s data, the licensee may seek the right to renew the contract for multiple renewal terms. In this case, the licensor may look to include automatic price increases as part of any renewal.

Termination
A data licensor often demands broad termination rights for the licensee's breach of the agreement and, in particular, the licensee's:

- Use of the data outside the permitted scope of licensed use.
- Failure to maintain data confidentiality and privacy.
- Failure to maintain the required data security protocols and procedures.

The licensor may also seek the right to terminate if the data licensee undergoes a change of control. What constitutes "control" should be specifically defined (see Assignment and Transferability).

A data licensee receiving data from a vendor may seek the right to terminate the license with or without cause on prior written notice to the vendor. This flexibility may be important for the licensee if at any time it no longer requires or desires to use the licensed data.

The parties should expressly provide for how the licensed data and the parties’ confidential information are to be handled on termination or expiration of the agreement, in particular, whether:

- The data and information should be returned to its owner or destroyed.
- Where the data licensee is a service provider that possesses the customer licensor’s data, the data should be retained by the licensee for temporary storage or migrated to the customer or a third-party service provider (see Data Migration and Transition).

The parties should also ensure that the agreement identifies any provisions that survive termination, such as:

- Confidentiality obligations.
- Payment obligations.
- Indemnity obligations
Confidentiality
The data licensor should ensure any agreement in which it licenses its data includes confidentiality obligations on the part of the licensee and that these obligations are consistent with the agreement's license obligations and restrictions.

Where the data licensee may share its own confidential information with the licensor, whether in the form of data or otherwise, mutual confidentiality obligations may be appropriate.

The parties should consider:

• The time limit on the confidentiality obligations. The data licensor should recognize that trade secret protection may be perpetual and therefore:
  • seek to carve out trade secrets from any time limit on data confidentiality; or
  • in any event, not curtail its trade secret rights with an unduly limited confidentiality sunset period (see Protecting Data as a Trade Secret).

• Whether to include common exceptions from the confidentiality requirements for information that is:
  • or becomes commonly known;
  • in the possession of the receiving party before disclosure;
  • separately received from a third party; or
  • independently developed by the receiving party.

• The standard and party bearing the burden of proof for showing that the confidentiality exception applies, whether by:
  • documentary evidence, which may be limited to evidence in existence before the disclosure; or
  • clear and convincing evidence.

• The treatment of legally compelled disclosure, including an obligation to notify the disclosing party and cooperate in seeking a protective order, and whether compulsorily disclosed information will:
  • no longer be confidential information and therefore not be subject to confidentiality requirements; or
  • remain confidential information, but which may be disclosed in this limited circumstance.

For more information concerning confidentiality agreements generally, see Practice Note, Confidentiality and Nondisclosure Agreements.

Assignment and Transferability
Licensees under copyright and patent license agreements generally cannot assign their rights under the agreement without the licensor’s consent. By contrast, a general commercial agreement is typically transferable by either party and the analysis for trade secrets may also differ. Therefore, whether a data license agreement is assignable by the licensee without the licensor's consent may depend on whether and how the data is protected as IP.

To remove doubt concerning the assignability of a data license, the parties should consider specifying in the agreement which rights and obligations are transferable and under what conditions. The data licensor generally will seek to limit the licensee's ability to assign the agreement without its consent. The data licensee usually will seek the right to transfer the agreement without consent either generally or under certain specified circumstances, such as to an affiliate or in connection with a merger, acquisition, asset sale or other corporate transaction.
Depending on the controlling jurisdiction, a narrowly-tailored restriction on assignment may not apply to a party's change of control or an assignment or transfer by merger or operation of law. The parties should therefore also consider expressly addressing whether these transactions are considered prohibited transfers under the agreement's anti-assignment clause. If so, a proposed change of control or merger, for example, may trigger:

- A termination right.
- A license fee increase or license "transfer" fee.
- A required assurance of performance and assumption of liability by the transferee or successor.
- Expanded license rights, which may depend on:
  - the transferee's or successor's financial stability
  - whether the transferee or successor is a competitor; or
  - the size of the transferee's or successor's resulting business.

For more information on the transferability of IP licenses and change-of-control provisions, see Practice Note, IP Licenses: Restrictions on Assignment and Change of Control.